Transforming regulatory compliance: A smarter approach to cybersecurity and privacy

Table of contents

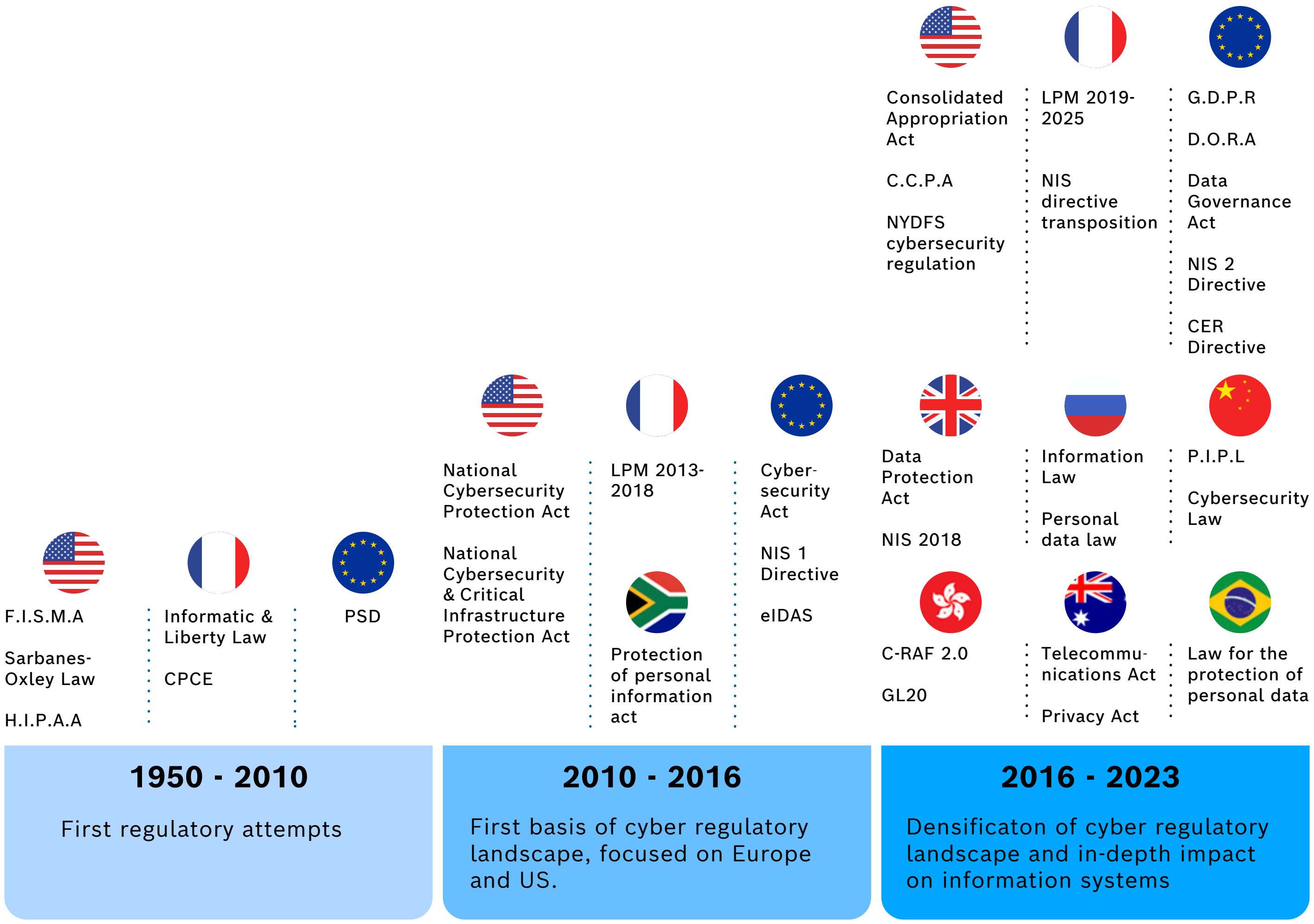
Executive summary

As technology rapidly evolves, companies struggle to keep up with ever-changing cybersecurity and data privacy rules. As Dara Warn, CEO of INE Security, aptly stated, “As cyber threats evolve, so do the regulatory frameworks designed to mitigate these risks. However, the complexity and diversity of these regulations can pose significant challenges for businesses aiming to fully comply with Governance, Risk and Compliance (GRC) standards.” [Source: *INE*]. Recent high-profile incidents, such as the $15.67 million fine imposed on Meta Platforms in November 2024 by South Korea’s Personal Information Protection Commission for unauthorized data collection and sharing [Source: *CampaignAsia*], highlight the profound risks organizations face without robust compliance frameworks.

Technology alone cannot account for the subtleties of regulatory language or emerging mandates. To address these challenges, a forward-thinking approach is essential—one that combines cutting-edge technology, comprehensive regulatory intelligence, and human expertise. This whitepaper outlines actionable recommendations and roadmaps to combine technological advancements with Human-in-the-Loop (HITL) oversight to ensure accurate and context-aware compliance management.

The compliance landscape: Growing complexity and need for innovation

As data-driven technologies become integral to business operations, the regulatory landscape for cybersecurity and privacy has grown increasingly complex. Regulations like the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States impose unique obligations and severe penalties for non-compliance. For instance, the European Union's Digital Markets Act (DMA) now requires tech giants like Apple to adapt their operating systems to ensure transparency and user rights, further emphasizing the growing regulatory pressure [Source: *European Commission*]. Non-compliance can lead to significant fines and long-lasting damage to a company's reputation, eroding customer trust. According to Wavestone's analysis, businesses are struggling with "hyper-growth" in regulatory requirements, creating additional layers of complexity that demand adaptability, proactive measures, and robust compliance frameworks (see Fig. 1) [Source: *Wavestone*]. This growing complexity underscores the need for intelligent tools and human oversight, making the HITL approach essential.



Consolidated Appropriation Act
C.C.P.A
NYDFS cybersecurity regulation
LPM 2019-2025
NIS directive transposition
G.D.P.R
D.O.R.A
Data Governance Act
NIS 2 Directive
CER Directive
F.I.S.M.A
Sarbanes-Oxley Law
H.I.P.A.A
Informatic & Liberty Law
CPCE
PSD
National Cybersecurity Protection Act
National Cybersecurity & Critical Infrastructure Protection Act
LPM 2013-2018
Protection of personal information act
Cyber-security Act
NIS 1 Directive
eIDAS
Data Protection Act
NIS 2018
C-RAF 2.0
GL20
Information Law
Personal data law
Telecommu-nications Act
Privacy Act
P.I.P.L
Cybersecurity Law
Law for the protection of personal data
1950 - 2010
First regulatory attempts
2010 - 2016
First basis of cyber regulatory landscape, focused on Europe and US.
2016 - 2023
Densificaton of cyber regulatory landscape and in-depth impact on information systems

Fig. 1 Evolution of cybersecurity regulatory landscape (Source: Wavestone)

Why regulatory intelligence is critical

To effectively address growing compliance complexities, organizations must invest in regulatory intelligence that keeps them informed and ahead of the curve. Reliable regulatory insights are essential for managing compliance risks, reducing the dependence on manual tracking, and ensuring transparency. This need for proactive, real-time regulatory insights forms the basis for our recommendations in the next section.

Introducing a forward-thinking approach to simplified regulatory compliance

We propose a compliance framework that enables organizations to navigate global cybersecurity and privacy regulations with confidence. This framework emphasizes actionable insights, user accessibility, and reliability as the foundation for a robust compliance strategy. Rather than presenting a fixed solution, this approach addresses regulatory challenges through innovative thinking, adaptive features, and a Human-in-the-Loop methodology that integrates technology with human judgment.

Core capabilities for addressing regulatory challenges

Our approach is centered on addressing industry pain points, such as those highlighted by Dara Warn: the ever-changing regulatory landscape, the difficulty of interpreting intricate legal requirements, and the operational strain of ensuring compliance across diverse jurisdictions [Source: *INE*]. We suggest that organization include these key capabilities in their compliance strategy:

1. Comprehensive regulatory coverage: Develop tools that aggregate and analyze regulatory data across global jurisdictions, offering clear insights into sector-specific mandates such as GDPR, CCPA, and emerging regulations like the Cyber Resilience Act (CRA).

2. User-friendly regulatory guidance: Create intuitive platforms catering to all levels—from entrepreneurs to compliance officers—with interactive features and sector-specific guidance that simplify complex compliance processes, enabling better decision-making.

2. Clause identification and simplification: Address the challenges of legal ambiguity by translating intricate clauses into understandable language, supplemented by practical examples to aid decision-making. For instance, the case of the $4.3 million fine imposed on the University of Texas M.D. Anderson Cancer Center due to regulatory misinterpretation highlights the importance of clarity in compliance understanding [Source: *Jones Walker*].

3. Reliability through metrics and human oversight: Integrate evaluation metrics like response accuracy checks, hallucination mitigation, and correctness validation, supported by HITL practices. This ensures that compliance recommendations are reliable and that risks associated with regulatory missteps are reduced.

A vision for scalable and adaptive compliance frameworks

Looking ahead, advanced scalable compliance frameworks that evolve with regulatory demands are essential for adapting to diverse regulatory landscapes.

1. Scalable solutions across sectors: Broaden applicability to industries like healthcare, finance, and retail, ensuring frameworks are flexible enough to address sector-specific nuances while remaining adaptable to emerging regulations like the Cyber Resilience Act (CRA).

2. Dynamic privacy and supply chain management: Address the growing need for privacy-first designs by introducing features like advanced Software Bill of Materials (SBOM) management that allow organizations to flag and curate vulnerable libraries in alignment with regulatory expectations.

3. Proactive compliance support with human oversight: Develop tools that provide real-time regulatory updates and guidance, with human experts to help organizations stay ahead of rapidly evolving mandates and interpret complex changes effectively.

Use cases: Addressing compliance challenges in the manufacturing sector

Entrepreneurs and Startups
Navigating complex product safety and cybersecurity regulations is critical for manufacturing startups. Regulations like the Cyber Resilience Act (CRA) demand thorough cybersecurity risk assessments throughout the product lifecycle, covering planning, design, development, production, and maintenance phases. Structured compliance frameworks provide clear guidance on mandatory requirements, ensuring safe product development and operational integrity.

Considering that the global smart manufacturing market is projected to grow at a CAGR of 13.2% from 2023 to 2030, how can startups leverage robust compliance frameworks to gain a competitive edge in this rapidly expanding market? [Source: GrandViewResearch]

Compliance officers
Compliance officers in manufacturing firms face challenges like adhering to global cybersecurity regulations such as the CRA, which mandates risk assessments, third-party component due diligence, and vulnerability management processes. A comprehensive compliance framework enables real-time regulatory updates, simplifies documentation processes, and streamlines auditing procedures, helping personnel reduce manual efforts and ensure alignment with evolving standards.

Under the CRA, failing to comply can lead to penalties of up to €15 million or 2.5% of global annual turnover. How can a proactive compliance strategy help compliance officers mitigate these risks while maintaining operational efficiency? [Source: TaylorWessing]

Regulatory experts
Regulatory experts in the manufacturing sector must interpret and implement complex cybersecurity regulations across diverse production facilities. The Human-in-the-Loop approach brings expert oversight to compliance, using precise tools to simplify regulations while keeping operations intact.

With automation and IoT driving rapid innovation in manufacturing, how can regulatory experts leverage adaptive compliance tools to enhance safety and operational compliance across global production networks? [Source: HighGear]

Use cases: Addressing compliance challenges across sectors

As cybersecurity regulations continue to evolve, industries beyond manufacturing face significant challenges in ensuring compliance while maintaining operational efficiency. This section highlights the specific challenges and opportunities within the energy utility and healthcare sectors, focusing on the unique regulatory landscapes these industries must navigate.

Energy and utility sector

Energy and utility companies must address growing cybersecurity threats to critical infrastructure while ensuring compliance with grid reliability standards like North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) and emissions regulations.

The global renewable energy market was valued at USD 1.21 trillion in 2023 and is expected to grow at a CAGR of 17.2% from 2024 to 2030. However, a significant number of energy professionals believe that cyber-attacks in the industry are a question of 'when', not 'if'. How can organizations proactively adapt to ensure compliance and resilience in an increasingly digital energy market? [Source: Grand View Research and Smart Energy International]

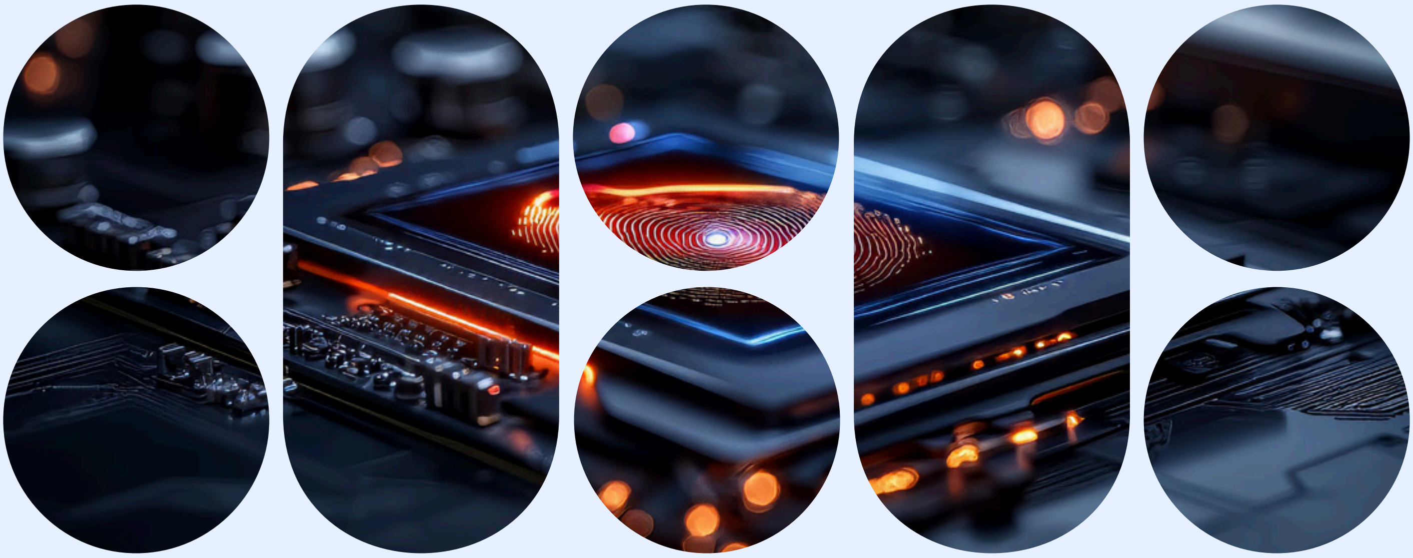
Tailored compliance frameworks help energy firms address risks such as grid vulnerabilities, secure energy transmission, and adherence to stringent emissions and cybersecurity standards. These frameworks empower organizations to enhance monitoring, reporting, and data security while aligning with global regulatory demands.

Healthcare sector

Healthcare organizations face mounting pressure to secure sensitive patient data while complying with regulations such as HIPAA, GDPR, and cybersecurity standards for medical devices. The rapid adoption of digital health technologies and telemedicine has expanded the attack surface, making compliance a critical priority for the sector.

Healthcare data breaches increased by 53.3% over the past three years, costing an average of $10.93 million per incident in 2023. How can healthcare providers mitigate risks and align with global cybersecurity regulations to protect patient trust? [Source: Resilientx]

Advanced compliance solutions help healthcare providers refine their cybersecurity strategies, adhering to regulations and safeguarding sensitive information. By implementing real-time guidance and risk management tools, organizations can address vulnerabilities while maintaining trust and operational integrity.
The HITL approach ensures that experts have the necessary context and human interpretation for accurate compliance implementation.



Approach to excellence: Advancing the future compliance framework

Looking ahead, the ability to anticipate regulatory changes will be a defining factor in organizational resilience. Forward-thinking compliance frameworks must not only keep pace with current mandates but also predict future shifts. By integrating proactive readiness measures, advanced privacy safeguards, and automated regulatory updates, organizations can position themselves to adapt swiftly to new requirements. This focus on agility and assurance enables businesses to streamline compliance processes, reduce operational risks, and build trust with stakeholders. Automated tracking and industry-specific adaptations ensure that compliance efforts are both efficient and effective, fostering accountability in an interconnected world. Ultimately, the goal is to help organizations navigate regulatory complexities while building resilience and accountability. By combining technology-driven insights with human expertise, businesses can achieve a balanced approach to compliance that addresses both immediate challenges and long-term goals. This framework empowers organizations to thrive amidst regulatory pressures, ensuring they remain compliant, competitive, and trusted by their stakeholders.

References

INE Security – CEO Dara Warn’s Insights on Regulatory Challenges.
CampaignAsia – Meta Platforms Fine for Unauthorized Data Collection.
European Commission – Digital Markets Act (DMA).
Wavestone – Analysis of the Cyber Regulatory Landscape.
McKinsey & Company – Importance of Regulatory Intelligence.
Jones Walker – University of Texas M.D. Anderson Cancer Center Case Study.
GrandViewResearch – Smart Manufacturing Market Growth Statistics.
TaylorWessing – Penalties Under the Cyber Resilience Act (CRA).
Resilientx – Healthcare Data Breach Statistics.

Author Details

Name: Sumitra Biswal
Department: Cybersecurity
Designation: Project Manager in the Intersection of AI and Cybersecurity